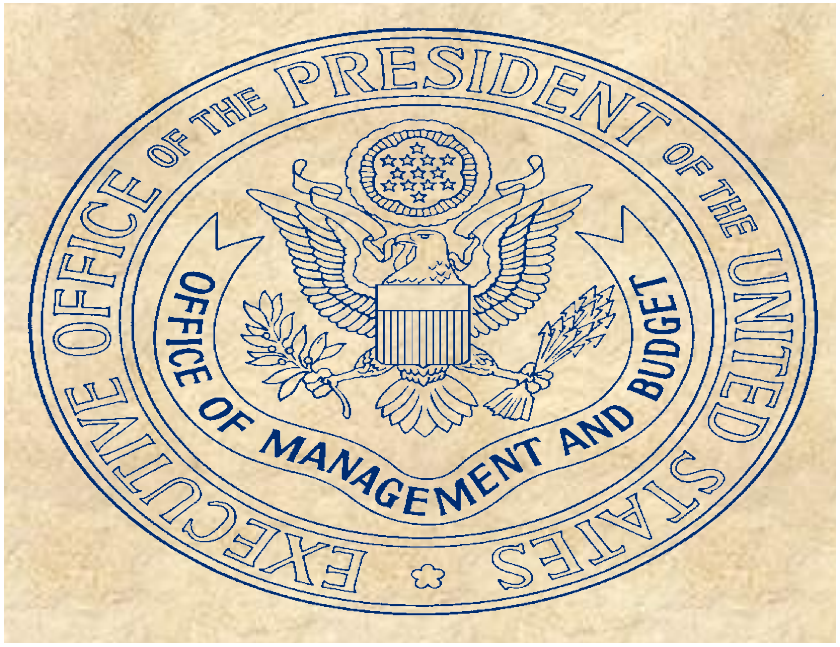
Electronic Government: Law, Policy, and Practice

Jonathan P. Womer
Information Policy and Technology
Office of Management and Budget
jwomer@omb.eop.gov

The Administration

The Administration's FY 2002 budget calls on agencies to create an electronic government that is:



- Citizen-Centered
- Results-Oriented
- Market-Based

The Administration . . .

The 2002 budget requests an e-government fund.

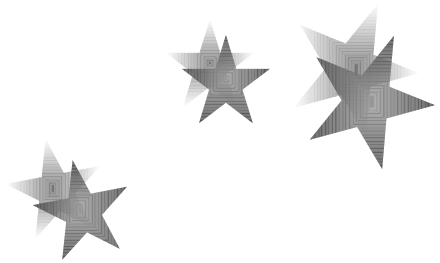
How the fund would work:

- $100 million, spreading this out over three years with a start of $20 million in FY 2002.
- Overseen by OMB similar to the process for the successful Y2K fund.
- Projects must use capital planning and have a business case.
- Projects must be interagency or infrastructure and must involve new innovation.
- Supports GPEA.

Government Paperwork Elimination Act (GPEA)

P.L. 105-277 (Title VII)

- **Agencies to automate interactions with outside partners/customers by October 2003 to the extent practicable.**
- **Electronic signatures should not be denied legal effect because electronic.**
- **Encourages electronic filing, electronic record keeping, and electronic signatures.**



Legal Effect and Validity

Electronic records submitted or maintained in accordance with procedures developed under this title, or electronic signatures or other forms of electronic authentication used in accordance with such procedures, shall not be denied legal effect, validity, or enforceability because such records are in electronic form.

-GPEA, section 1707

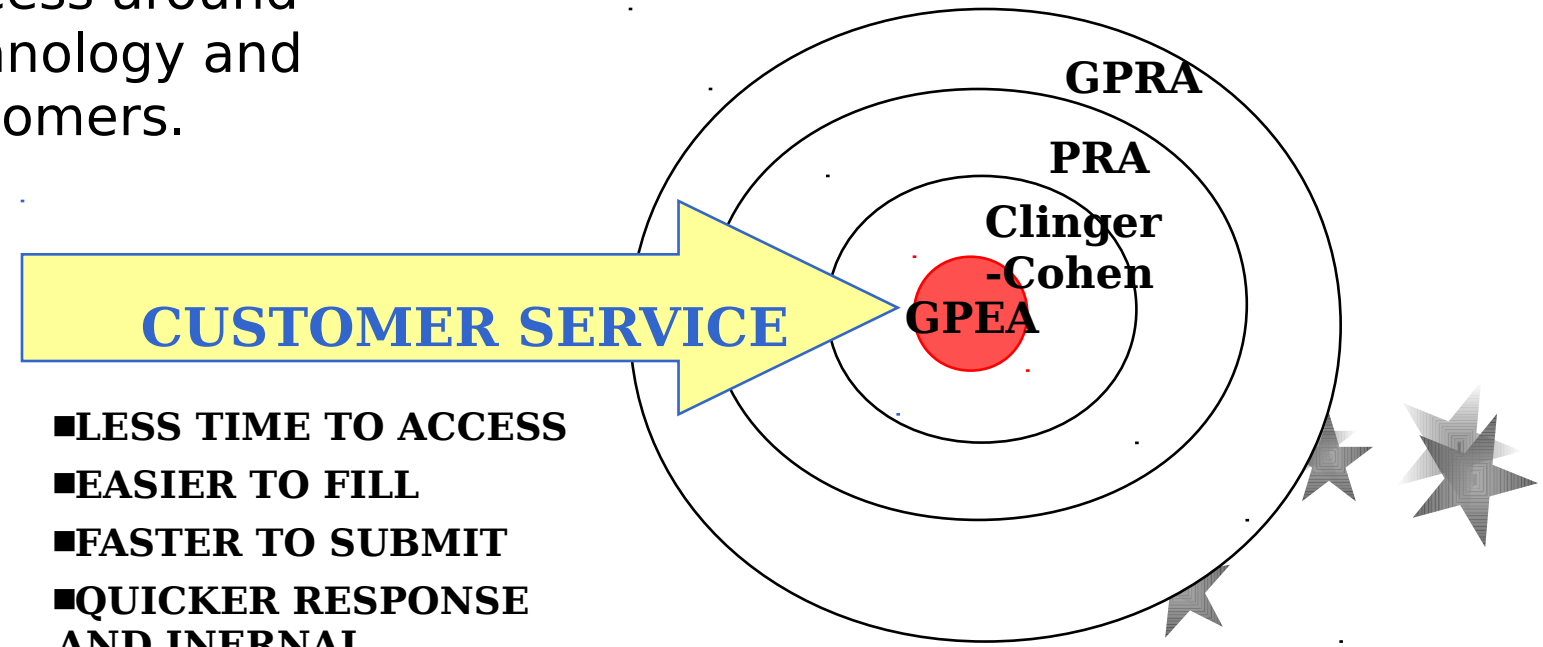
E-SIGN PL 106-229

- **Effective as soon as October 1 2000.**
- **Primarily commercial transactions.**
- **Government: When regulating, when market participant, and special cases.**
- **Not Contracts.**
- **Reinforces electronic signatures and GPEA.**

Other Legislation

- Provide customer service in a fundamentally better way
- Re-engineer business process around technology and customers.

When we combine these laws we get:

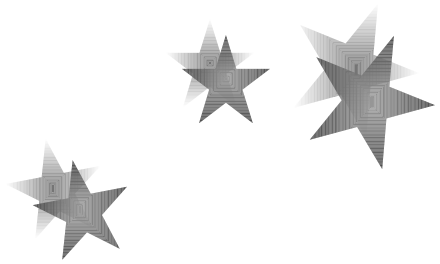


- **LESS TIME TO ACCESS**
- **EASIER TO FILL**
- **FASTER TO SUBMIT**
- **QUICKER RESPONSE AND INERNAL PROCESSING**

OMB's GPEA Guidance

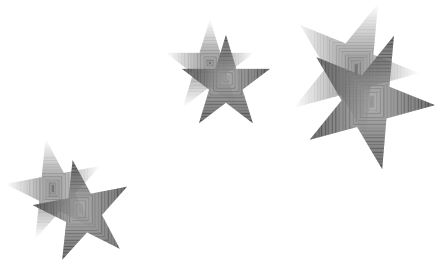
i.e. "How to go electronic"

- **Final OMB guidance: Federal Register Vol. 65, No. 85 - 25508–25521 [00–10801]**
- **http://www.whitehouse.gov/omb/memoranda/m00-10.html**
- **Also, NIST/PKI, DOJ, Treasury, NARA**



OMB's Guidance on Going Electronic

- **Weigh the magnitude of the risk and select an appropriate combination of technology and practice to cost-effectively minimize risk and maximize benefits to agency and to customers.**
- **Use electronic signatures to reduce burden.**
- **Incorporate security into information and systems architecture.**



OMB's Guidance on Going Electronic - continued

- **Plans on agency implementation were due to OMB 31 October 2000 (and OMB tracking through information collection review process defined by Paperwork Reduction Act).**
- **Funding requirements for GPEA projects should be noted in IT Capital Asset Plans sent to OMB.**
- **" . . . develop baselines and verifiable performance measures that track the agency's mission, strategic plans, and tactical goals, as required by the Clinger-Cohen Act."**

Authentication/Identity Techniques

- ***Personal Identification Numbers (PINS)***

  Automated teller machines (with token)

  IRS TeleFile, SEC EDGAR (without token)

- ***Cryptographic Digital Signatures***

  Public and private sector pilots, some production applications

- ***Biometrics***

  Can be used in conjunction with digital signatures

How do they differ?

- **PINs and biometrics/signature dynamics tend to be one to one within a single application, i.e. automates the stovepipes.**

- **Cryptographic digital signatures can be used for multiple applications utilizing digital certificates as a component of a Public Key Infrastructure, i.e. can cut across stovepipes.**

Privacy Act (5 U.S.C. 552a)

- **Federal databases containing personal identifying information in support of PINs, biometrics, or digital signatures are "systems of records."**

- **Contractor-maintained databases containing personal identifying information, e.g. contracted CA/RA services, are usually covered "systems of records." Possible exception if certificates are generally available, e.g. SET.**

Practical Implications/Good Practices

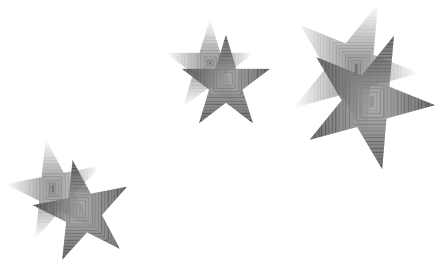
- **Collect it only if you need it. [sec 1708 of GPEA]**
- **Often system of records under Privacy Act**
- **Disclose conditions and limits of use and Articulate and disclose protective policies and measures: -- POST PRIVACY POLICY**
- **Provide reasonable personal access with ability to correct and/or update.**
- **Destroy personal information when no longer needed; important to determine appropriate retention period.**

The bottom line:

Designing an automated system that is more efficient, with better authentication and privacy than paper-based systems is not difficult,

BUT…

You must cover all the bases.



Electronic Commerce Sources

- **Electronic Government at the CIO Council**
  http://cio.gov
- **"Framework for Global Electronic Commerce"**
  http://www.ecommerce.gov
- **GPEA Resources**
  http://cio.gov/egov/projects/gpea/
  gpea_index.htm
- **Federal Public Key Infrastructure Steering Committee**
  http://cio.gov/fpkisc